

ISMAIL J. RAMSEY (CABN 189820)
United States Attorney

MARTHA BOERSCH (CABN 126569)
Chief, Criminal Division

CHRISTIAAN HIGHSMITH (CABN 296282)
DAVID WARD (CABN 239504)
Assistant United States Attorneys

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-7200
FAX: (415) 436-7230
christiaan.highsmith@usdoj.gov
david.ward@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA,)	NO. CR 20-00249 RS (LB)
)	
Plaintiff,)	
)	UNITED STATES' OPPOSITION TO
v.)	DEFENDANT ANDRADE'S MOTION
)	REGARDING REVIEW OF SEIZED EVIDENCE
)	FROM TREZOR WALLETS
MARCUS ANDRADE)	
)	Hearing Date; May 5, 2024
Defendant.)	Court: Hon. Laurel Beeler, Courtroom B, 15 th Fl.
)	

I. INTRODUCTION

Defendant Marcus Andrade has filed a Motion asking this Court to enforce its March 17, 2024 Order allowing him access to data from four Trezor wallets (similar to encrypted hard drives) seized pursuant to a lawful search warrant in the Southern District of Texas. *Dkt. 297*. In his Motion, Andrade proposes to bring an expert to attach the wallets to his or her computer, access the evidence without providing the government any access, unilaterally inspect the evidence while keeping the contents secret from the government, copy and take whatever he sees fit from those devices, then to re-password protect them so the government cannot access the data. And Andrade refuses to provide the government with

any evidence he take. This was not what he sought in his Motion to Compel, and not what the Court ordered. More fundamentally, courts have repeatedly rejected exactly what Mr. Andrade proposes here.

I. ARGUMENT

1. The government cannot be compelled to produce data from the encrypted Trezors

On January 24, 2024, defendant Andrade filed a discovery motion seeking a Court order, pursuant to Rule 16(a)(1)(E) and *Brady*, to, among many other things, inspect four Trezor wallets seized by the government in 2020 in the Southern District of Texas. Defendant Andrade's motion demanded that "the government either produce the images it has taken of the data on those Trezor wallets, or, alternatively, to permit Mr. Andrade's counsel to send someone to inspect the Trezor wallets and make images of all of the digital currency transactional data on the wallets." *Dkt. 275* (Def. Third Mot. to Compel). In his motion to compel, defendant Andrade asserted, wrongly, that "the government declined to produce data from the Trezor wallets." *Id.* This is not true. The government has repeatedly told the defendant that it has not been able to access the Trezor wallets, and cannot do so without a password, and therefore has no data from the wallets. Defendant was well aware the government did not have any data from the Trezors, yet he still filed a motion asking the Court to compel the government to "produce the images it has taken of the data on those Trezor wallets." *Id.*

Rule 16 does allow a defendant to "inspect and copy" tangible items in the government's "possession, custody, or control," that may be material to his defense. Based on that, the Court ordered the government to provide the defendant with access to the Trezors, which allows him to "inspect and copy" evidence in the government's possession. *Dkt. 292* (Order on Motion). Following the Court's order, the government agreed to allow the defendant to access the Trezor wallets and to copy transactional data. But to do so, the government needs the password, and defendant Andrade continues to refuse to provide it. Instead, defendant Andrade demands that he be given unilateral access to the wallets to inspect, image, and copy data in secret. Andrade has stated that he is not required to, and will not, provide the government access to, or a copy of, any of that information.

In his motion here, Andrade asserts, without citing to a single case or other legal authority, that "*Rule 16(a)(1)(E) expressly requires the government to allow the defendant to inspect and copy the Trezors, without any requirement that he share what he obtains.*" *Dkt. 297* (Motion to Enforce Order).

1 Defendant Andrade's statement is wrong. He misstates the law and fails to acknowledge or address
2 significant legal authority directly contrary to his assertion.

3 Courts have repeatedly held that data or information on an encrypted device is not within the
4 government's "custody or control" and therefore the government cannot be compelled to produce it
5 under Rule 16(a)(1)(E) when a defendant refuses to provide his password. *See e.g. United States v.*
6 *Young*, 2024 WL 913308 * 4 (D. Minn, 2024). *Young* is particularly illustrative. In *Young*, as here, the
7 defendant moved the court for an order requiring the government to permit defense counsel to inspect a
8 cellphone which was in the government's possession. *Id.* ("Young moves the Court to enter an order
9 requiring the Government to permit defense counsel to inspect a cellphone, which is presently in the
10 Government's custody pursuant to a search warrant issued by this Court. The Government has not been
11 able to access the cellphone's data because it is encrypted."). And as here, the defendant in *Young*
12 refused to provide the government his password and declined to allow the government access. *Id.*
13 ("Young does not propose or agree that the government could access the cellphone as part of his
14 proposed inspection and declined to provide the necessary password.").

15 The court in *Young* denied defendant's motion. *Id.* ("Young cites no authority for the
16 proposition that a defendant in a criminal case may not only unlock a device the Government has been
17 unable to decrypt for inspection and copying, but then lock it back up when complete—even though
18 there is a warrant authorizing a search of the device. The Court declines to permit Young's inspection of
19 the cellphone on such terms."). The court's rationale in *Young* was clear:

20 "Rule 16(a)(1)(E) provides: 'the government must permit the defendant to inspect and to
21 copy or photograph books, papers, documents, data, photographs, tangible objects,
22 buildings or places, or copies or portions of any of these items, if the item is within the
23 government's possession, custody, or control.'" Fed. R. Crim. P. 16(a)(1)(E). While the
24 physical cellphone is the Government's possession by virtue of a warrant, the data it
25 contains is not in the Government's possession because the cellphone is encrypted, Young
has refused to provide his passcode, and the Government has not been able to break the
encryption. Consequently, the data on the cellphone do not fall within the scope of Rule
16(a)(1)(E). Similarly, there is no obligation under *Brady* requiring the Government to
discover information not in its possession."

26 *Id.*, citing *United States v. Jones*, 34 F.3d 596, 599 (8th Cir. 1994) ("*Brady* requires the prosecution to
27 disclose to the defendant only evidence in the prosecution's possession.")
28

1 The court, in *United States v. Norman Gray*, reached the same conclusion, and noted the
2 significant legal support for its position. 2024 WL 1526368 (S.D.N.Y. April 9, 2024). The court in
3 *Gray* held that “as courts have uniformly held, the contents of an encrypted device are not within the
4 government’s possession, custody, or control for purposes of Rule 16 or *Brady*.” *Id.*, citing *Young*, and
5 *United States v. Case*, 2020 WL 4227554, at *3 (D. Idaho July 23, 2020). The court in *Gray* noted that
6 the government was willing to provide the defendant with access to an image of the phone under Rule
7 16 if the defendant first provided a password, but the defendant had refused. *Id.* The court in *Gray*
8 stated that, while “under the Fifth Amendment, it is Gray’s right to decline to give the government this
9 information, he may not seek to access the phone’s data while denying the same access to the
10 government.” *Id.*, citing *Young*, 2024 WL 913308 *5. The court in *Gray* stated that is was “unaware of
11 any authority, under Rule 16 or *Brady*, that requires the government to give superior access to evidence
12 than the government itself has.” *Id.*, citing *United States v. Bibby*, 752 F.2d 1116, 1125 (6th Cir. 1985).

13 Courts in the Ninth Circuit has similarly held that encrypted data on an electronic device is not
14 within the government’s custody and control. *See Case*, 2020 WL 4227554 (D. Idaho, July 23, 2020),
15 *aff’d* 851 F. Appx. 105 (9th Cir. 2021) (“the Government was not obligated to disclose the FBI’s
16 possession of the cellphone or produce its contents to the defense. Because the phone was password-
17 protected, the Government did not have access to the records the defendant seeks. The Government
18 could not suppress evidence they did not have access to.”). The court in *Case* held that the defendant
19 had no *Brady* or Rule 16 right to either his hardware or its encrypted contents. *Id.*

20 Similarly, in *United States v. Sullivan*, the defendant sought allegedly exculpatory text messages
21 and emails on an encrypted Cellebrite extraction from her iPhone. 2020 WL 5351030, at *1, 6 (D. Haw.
22 Sept. 4, 2020). But, like defendant Andrade here, Sullivan refused to provide the government with the
23 passcode to decrypt and access the data. *Id.* The court held that the defendant “cannot both refuse to
24 provide the passcode required to access [her] iPhone[]’s encrypted information and simultaneously
25 claim that the information is unavailable to her.” *Id.* The court in *Sullivan* explained that while the
26 defendant “is under no obligation to provide the government with the passcode to [her] iPhone[]”—at
27 least without an All Writs Act order—“she cannot complain that the government is withholding
28 information from her when she alone is able to provide a passcode to access that very information.” *Id.*

1 The caselaw on this issue is clear. Defendant Andrade can provide the government with the
 2 password to the Trezor wallets. If he choses to do so, the government can and will image the devices
 3 and provide the defendant with a copy. If he does not, he cannot compel this Court to order the
 4 government to provide him with unilateral access to the devices.

5 **2. The Government is Not Seeking Defendant's Password**

6 Defendant claims that the government cannot compel the defendant to provide the government
 7 the password to his Trezor wallets or to compel him to decrypt the devices without violating his Fifth
 8 Amendment privilege. *Dkt.* 297. That is not always true. *See e.g., United States v. Spencer*, 2018 WL
 9 1964588, (N.D. Cal. 2018). But it is irrelevant here, as the government is not seeking to compel the
 10 defendant to produce passwords to the Trezor wallets. The government simply notes that without the
 11 passwords, it is unable to access the data that the defendant demands to inspect and copy, and so in those
 12 circumstances, any data on the Trezor wallets is not in the government's possession, custody, or control
 13 and cannot be produced pursuant to Rule 16 or *Brady*.

14 **3. The Government's Access to the Devices Under the Fourth Amendment has not Expired and is Irrelevant to Defendant's Motion**

15 Defendant next asserts that "as the government has repeatedly argued itself as to other devices,
 16 more than four years after it seized the Trezors, it no longer has lawful access to the device under the
 17 Fourth Amendment." *Dkt.* 297. This is another misrepresentation. While the government has
 18 voluntarily returned some electronic devices to the defendant, the government has never "argued itself"
 19 that it no longer has lawful access or probable cause under the Fourth Amendment to access the Trezors.
 20 Nor does it do so here. In fact, there is significant legal authority for the position that the government
 21 still has probable cause and Fourth Amendment authority to access the Trezor wallets. *See, e.g., United*
 22 *States v. Flores*, 802 F.3d 1028, 1043 (9th Cir. 2015) (explaining that the mere passage of substantial
 23 amounts of time is particularly immaterial with electronic evidence); *United States v. Magana*, 2022 WL
 24 4237547, at *6 (E.D. Cal. Sept. 14, 2022) (collecting cases holding that multi-year "delays due to the
 25 government's inability to obtain access to data from electronic devices, whether due to encryption or an
 26 inability to access a locked cell phone, have been found to be reasonable under the Fourth
 27 Amendment"); *United States v. Sosa*, 379 F. Supp. 3d 217, 222 (S.D.N.Y. 2019) (similar).

Defendant's sole support for his claim that the government's access to the devices under the Fourth Amendment has expired is a citation to *United States v. Kopankov*, 672 F. Supp. 3d 862 (N.D. Cal. 2023). But that case involved a search in the Northern District of California in violation of the search warrant's "Attachment C," a time-limiting requirement to searching electronic devices unique to the Ninth Circuit. *Id.* at 867–68. The *Kopankov* court's reasoning hinged on the expiration of the Attachment C deadline, for after that deadline, "the government was not operating pursuant to a valid warrant." *Id.* at 867. But the warrant in this case was executed in the Southern District of Texas, pursuant to a warrant without an Attachment C. Defendant Andrade does not explain or address this distinction between *Kopankov* and this case.

But again, that issue is irrelevant to defendant's Motion under Rule 16. The remedy for a violation of the Fourth Amendment is suppression of any evidence obtained in violation thereof, not as a justification to allow a defendant to have unsupervised access to unilaterally search and take electronic data on devices lawfully seized by the government. Defendant cites no authority for his argument that, even if the government's authority under the Fourth Amendment to search the devices has expired, how that allows him to unilaterally access the devices, image, copy, or otherwise inspect, and to do so outside the presence of the government.

4. The Defendant has not made his required showing that Data on the Trezors is *Brady* or Material to his defense.

In addition to Rule 16's other requirements, a defendant is required to make a specific showing that the information he seeks is material to his defense or is potential *Brady*. See e.g. *United States v. Jordan*, 316 F.3d 121, 135 (11th Cir. 2003). In *Jordan*, the Eleventh Circuit held that "general description is insufficient; rather, the defendant must provide a specific explanation of how the evidence will be 'helpful to the defense.'" *Id.*, citing *United States v. Marshall*, 132 F.3d 63, 67–68 (D.C. Cir. 1998) ("helpful" means relevant to preparation of the defense and not necessarily exculpatory); *United States v. Olano*, 62 F.3d 1180, 1203 (9th Cir.1995). As the Fifth Circuit held in *United States v. Buckley*, 586 F.2d 498, 506 (5th Cir. 1978), quoting *United States v. Ross*, 511 F.2d 757, 762–63 (5th Cir.1975), the defendant must "show" "more than that the [item] bears some abstract logical relationship to the issues in the case.... There must be some indication that the pretrial disclosure of the [item] would

1 ... enable [] the defendant significantly to alter the quantum of proof in his favor.”

2 Defendant Andrade has not stated with any specificity how access to cryptocurrency
3 transactional data presumably stored on the Trezor wallets is either potential *Brady* or specifically how it
4 may be helpful to his defense. He must do so, and he must provide some specific rationale for the
5 requirement that disclosure would be helpful to the defense.

6 **III. CONCLUSION**

7 Defendant’s Motion is but the latest in a relentless salvo of discovery motions and letters filed in
8 this case. Defendant’s motion to “enforce” the Court’s order misstates his earlier position and
9 misrepresents the government’s position. Most troubling, defendant Andrade seeks an order from this
10 Court which would run counter to significant precedent, yet fails to provide any legal support for his
11 request, or to address or even acknowledge significant caselaw that holds contrary to his position. The
12 Court should deny defendant’s motion.

13
14 DATED: April 22, 2024

Respectfully submitted,

15 ISMAIL J. RAMSEY
16 United States Attorney

17 /s/ David J. Ward
18 DAVID J. WARD
19 CHRISTIAAN HIGHSMITH
Assistant United States Attorneys
20 MATTHEW CHOU
Special Assistant United States Attorney
21
22
23
24
25
26
27
28